WHAT IS CLAIMED IS:

1. A filtering apparatus which is interposed between a client and a server providing a service in accordance with each of access requests from the client, and which transmits only a legal access request among the access requests to the server, the filtering apparatus comprising:

an illegal pattern database which stores patterns of illegal accesses to the server;

a pattern estimation unit which estimates legality of each of the access requests based on the illegal access patterns stored in the illegal pattern database and on a predetermined pattern estimation rule; and

a pattern determination unit which determines whether each of the access requests is to be transmitted to the server based on the estimation by the pattern estimation unit and on a predetermined pattern determination rule.

2. The filtering apparatus according to claim 1, wherein

the pattern estimation unit estimates that each of the access requests is an illegal access if the access request corresponds to any one of the illegal access patterns stored in the illegal pattern database, and estimates that the access request is a legal access if the access request does not correspond to any one of the illegal access patterns stored in the illegal pattern database; and

the pattern determination unit determines that the access request estimated as the illegal access by the pattern estimation unit is not to be transmitted to the server, and determines that the access request estimated as the legal access by the pattern estimation unit is to be transmitted to the server.

3. The filtering apparatus according to claim 1, wherein

the pattern estimation unit calculates a predetermined estimation value according to a degree to which each of the access requests corresponds to the illegal access patterns stored in the illegal pattern database; and

the pattern determination unit compares the estimation value calculated by the pattern estimation unit with a predetermined threshold value, and determines whether the access request is to be transmitted to the server.

4. The filtering apparatus according to claim 1, further comprising:

a legal pattern database which stores patterns of legal accesses to the server; and

a predetermination unit which predetermines whether each of the access requests corresponds to any one of the legal access patterns stored in the legal pattern database before the estimation unit estimates the legality of the

access request,

wherein the pattern estimation unit estimates the legality of only the access request determined not to correspond to any one of the legal access patterns by the predetermination unit.

5. The filtering apparatus according to claim 1, further comprising a external transmission unit which transmits each of the access requests determined not to be transmitted to the server by the pattern determination unit, to a predetermined external device based on a predetermined external transmission rule.

6. The filtering apparatus according to claim 1, further comprising a storage unit which stores each of the access requests determined not to be transmitted to the server by the pattern determination unit, in a predetermined storage medium based on a predetermined storage rule.

7. The filtering apparatus according to claim 1, further comprising a update unit which updates the illegal pattern database, the legal pattern database, the pattern estimation rule, the pattern determination rule, the external transmission rule, the storage rule, or a predetermined update rule, based on the predetermined update rule.

8. The filtering apparatus according to claim 1, further comprising:

a statistically illegal request database which stores information on the access requests considered to be illegal accesses from the statistic of the access requests for the server;

a statistic estimation unit which estimates the legality of each of the access requests based on the information stored in the statistically illegal request database and on a predetermined statistic estimation rule;

a statistic determination unit which determines whether the access request is to be transmitted to the server based on the estimation result of the estimation unit and on a predetermined determination rule; and

an access request transmission unit which transmits, as a legal access request, only the access request determined to be transmitted to the server by the pattern and statistic determination units, to the server.

9. The filtering apparatus according to claim 8, wherein

the statistically illegal request database stores transmitting end information on the clients each of which issues access requests within a predetermined time, the number of the access requests exceeding a predetermined number, among the clients who transmit the access requests

to the server;

the statistic estimation unit estimates that each of the access requests is the illegal access if the transmitting end information on the access request corresponds to any one of the transmitting end information stored in the statistically illegal request database, and estimates that the access request is the legal access if the transmitting end information on the access request does not correspond to any one of the transmitting end information stored in the statistically illegal request database; and

the statistic determination unit determines that the access request estimated as the illegal access by the statistic estimation unit is not to be transmitted to the server, and determines that the access request estimated as the legal access by the statistic estimation unit is to be transmitted to the server.

10. The filtering apparatus according to claim 8, wherein

the statistically illegal request database stores request contents of the access requests within a predetermined time, the number of the access requests of each request content exceeding a predetermined number, among request contents of the access requests transmitted to the server;

the statistic estimation unit estimates that the

access request of each of the access requests is the illegal access if the request content of the access request corresponds to any one of the request contents stored in the statistically illegal request database, and estimates that the access request is the legal access if the request content of the access request does not correspond to any one of the request contents stored in the statistically illegal request database; and

the statistic determination unit determines that the access request estimated as the illegal access by the statistic estimation unit is not to be transmitted to the server, and determines that the access request estimated as the legal access by the statistic estimation unit is to be transmitted to the server.

11. The filtering apparatus according to claim 8, wherein

the statistically illegal request database stores transmitting end information on the clients each of which issues access requests, the number of which exceeds a predetermined number within a predetermined time, among the clients who transmit the access requests to the server, and stores request contents of the access requests, the number of which exceeds a predetermined number within a predetermined time, among the request contents of the access requests transmitted to the server;

the statistic estimation unit estimates that each of the access requests is the illegal access if the transmitting end information on the access request corresponds to any one of the transmitting end information stored in the statistically illegal request database or the request content of the access request corresponds to any one of the request contents stored in the statistically illegal request database, and estimates that the access request is the legal access if the transmitting end information on the access request does not correspond to any one of the transmitting end information stored in the statistically illegal request database and the request content of the access requests does not correspond to any one of the request contents stored in the statistically illegal request database; and

the statistic determination unit determines that the access request estimated as the illegal access by the statistic estimation unit is not to be transmitted to the server, and determines that the access request estimated as the legal access by the statistic estimation unit is to be transmitted to the server.

12. The filtering apparatus according to claim 8, wherein the statistically illegal request database stores transmitting end information on the clients each of which issues access requests, the number of which exceeds a

predetermined number within a predetermined time, among the clients who transmit the access requests to the server, and stores request contents of the access requests, the number of which a predetermined number within a predetermined time, among the request contents of the access requests transmitted to the server;

the statistic estimation unit calculates a predetermined estimation value according to a degree to which the transmitting end information on each of the access requests and the request content of the access request correspond to the transmitting end information and the request contents stored in the statistically illegal request database, respectively; and

the statistic determination unit compares the estimation value calculated by the statistic estimation unit with a predetermined threshold value, and determines whether the access request is to be transmitted to the server.

13. The filtering apparatus according to claim 8, wherein the statistic estimation unit estimates the legality of only the access request determined to be transmitted to the server by the pattern determination unit.

14. The filtering apparatus according to claim 8, wherein the pattern estimation unit estimates the legality of only the access request determined to be transmitted to the server by the statistic determination unit.

15. The filtering apparatus according to claim 8, wherein the predetermination unit predetermines whether only the access request determined to be transmitted to the server by the statistic determination unit corresponds to any one of the legal access patterns stored in the legal pattern database.

16. The filtering apparatus according to claims 8, further comprising a external transmission unit which transmits the access requests which are not transmitted to the server by the access request transmission unit, to the predetermined external device based on a predetermined external transmission rule.

17. The filtering apparatus according to claim 8, further comprising a storage unit which stores the access requests which are not transmitted to the server by the access request transmission unit, to the predetermined storage medium based on a predetermined storage rule.

18. The filtering apparatus according to claim 8, further comprising a update unit which updates the statistically illegal request database, the statistic estimation rule, the statistic determination rule, the external transmission rule, and at least one of the storage rule and a predetermined update rule, based on at least one of the predetermined update rule and the statistic of the access requests to the server.

19. The filtering apparatus according to claim 18, wherein the update unit performs any one or both of addition and deletion of at least one of the transmitting end information and the request contents stored in the statistically illegal request database, according to any one or both of the number of access requests for each client who transmits the access requests to the server within the predetermined time and the number of access requests for each request content of the access requests transmitted to the server within the predetermined time.

20. The filtering apparatus according to claim 1, further comprising:

an illegal response database which stores patterns of illegal responses which should not be transmitted to each of the clients among the responses transmitted from the server to each of the clients as the service in accordance

with the respective access requests;

a response estimation unit which estimates the legality of each of the responses based on the illegal response patterns stored in the illegal response database and a predetermined response estimation rule;

a response determination unit which determines whether the response is to be transmitted to the client based on an estimation result of the response estimation unit and on a predetermined response determination rule; and

a response transmission unit which transmits, as a legal response, only the response determined to be transmitted to the client by the response determination unit, to the client.

21. The filtering apparatus according to claim 20, wherein

the response estimation unit estimates that the response is an illegal response if the response corresponds to any one of the illegal response patterns stored in the illegal response database, and estimates that the response is a legal response if the response does not correspond to any one of the illegal response patterns stored in the illegal response database; and

the response determination unit determines that the response estimated as the illegal response by the response estimation unit, is not to be transmitted to the client,

and determines that the response estimated as the legal response by the response estimation unit, is to be transmitted to the client.

22. The filtering apparatus according to claim 20, wherein

the response estimation unit calculates a predetermined estimation value according to a degree to which the response corresponds to the illegal response patterns stored in the illegal response database; and

the response determination unit compares the estimation value calculated by the response estimation unit with a predetermined threshold value, and determines whether the response is to be transmitted to the client.

23. The filtering apparatus according to claim 20, further comprising an external transmission unit which transmits at least one of the response that is not transmitted to the client by the response transmission unit and the access request causing the response, to a predetermined external device based on a predetermined external transmission rule.

24. The filtering apparatus according to claim 20, further comprising an storage unit which stores at least one of the response that is not transmitted to the client by the response transmission unit and the access request causing the response,

in the predetermined storage medium based on a predetermined storage rule.

25. The filtering apparatus according to claim 20, further comprising an update unit which updates the illegal response database, the response estimation rule, the response determination rule, the external transmission rule, and at least one of the storage rule and a predetermined update rule, based on a predetermined update rule.

26. The filtering apparatus according to claim 1, further comprising an access request decryption unit which decrypts an access request which has been subjected to a predetermined encryption processing,

wherein the pattern estimation unit, the predetermination unit or the statistic estimation unit estimates or determines the access request decrypted by the access request decryption unit.

27. The filtering apparatus according to claim 26, wherein if only the legal access request among the access requests is to be transmitted to the server, not the access request decrypted by the access request decryption unit but the access request which has been subjected to the predetermined encryption processing is transmitted to the server.

28. The filtering apparatus according to claim 26, further comprising a response decryption unit which decrypts a response which has been subjected to a predetermined encryption processing, wherein the response estimation unit estimates the response decrypted by the response decryption unit.

29. The filtering apparatus according to claim 28, wherein if only the legal response among the responses is to be transmitted to the client, not the response decrypted by the response decryption unit but the response which has been subjected to the predetermined encryption processing is transmitted to the client.

30. The filtering apparatus according to claim 1, further comprising:

a pseudo-response database which stores pseudo-responses corresponding to the patterns of the illegal accesses to the server, respectively, and each indicating that the corresponding illegal access is successful or successfully proceeding;

a pseudo-response creation unit which creates pseudo-responses corresponding to the patterns of the access requests, each of which is determined as the illegal access and is not transmitted to the server, respectively while

referring to the pseudo-response database; and

a pseudo-response transmission unit which transmits the pseudo-responses created by the pseudo-response creation unit to the clients, respectively.

31. The filtering apparatus according to claim 1, further comprising:

a decoy unit which receives the access requests each of which is determined as the illegal access and is not transmitted to the server, and creates, as a decoy of the sever, pseudo-responses each indicating that the corresponding illegal access is successful or successfully proceeding; and

a pseudo-response transmission unit which transmits the pseudo-responses created by the decoy unit to the clients, respectively.

32. The filtering apparatus according to claim 1, further comprising:

a pseudo-response database which stores pseudo-responses corresponding to the patterns of the illegal accesses to the server, respectively, and each indicating that the corresponding illegal access is successful or successfully proceeding;

a pseudo-response creation unit which creates

pseudo-responses corresponding to the illegal access patterns stored in the pseudo-response database among the access requests each of which is determined as the illegal access and is not transmitted to the server;

a decoy unit which receives the access requests which do not correspond to the illegal access patterns stored in the pseudo-response database among the access requests each of which is determined as the illegal access and is not transmitted to the server, and creates, as a decoy of the sever, pseudo-responses each indicating that the corresponding illegal access is successful or successfully proceeding; and

a pseudo-response transmission unit which transmits the pseudo-responses created by the pseudo-response creation unit or the decoy unit to the clients, respectively.

33. A filtering method used on a client and a server providing a service in accordance with each of access requests from the client, and which transmits only a legal access request among the access requests to the server, the method comprising:

a pattern estimation step of referring to an illegal pattern database which stores patterns of illegal accesses to the server, and estimating legality of each of the access requests based on the illegal access patterns referred to

and on a predetermined pattern estimation rule; and

a pattern determination step of determining whether each of the access requests is to be transmitted to the server based on an estimation result at the pattern estimation step and on a predetermined pattern determination rule.

34. The filtering method according to claim 33, wherein

the pattern estimation step includes estimating that each of the access requests is an illegal access if the access request corresponds to any one of the illegal access patterns stored in the illegal pattern database, and estimating that the access request is a legal access if the access request does not correspond to any one of the illegal access patterns stored in the illegal pattern database; and

the pattern determination step includes determining that the access request estimated as the illegal access in the pattern estimation step is not to be transmitted to the server, and determining that the access request estimated as the legal access in the pattern estimation step is to be transmitted to the server.

35. The filtering method according to claim 33, wherein

the pattern estimation step includes calculating a predetermined estimation value according to a degree to which each of the access requests corresponds to the illegal access

patterns stored in the illegal pattern database; and

the pattern determination step includes comparing the estimation value calculated in the pattern estimation step with a predetermined threshold value, and determining whether the access request is to be transmitted to the server.

36. The filtering method according to claim 33, further comprising a predetermination step of referring to a legal pattern database which stores patterns of legal accesses to the server, and determining whether each of the access requests corresponds to any one of the legal access patterns stored in the legal pattern database before the legality of the access request is estimated in the estimation step,

wherein the pattern estimation step includes estimating the legality of only the access request determined not to correspond to any one of the legal access patterns in the predetermination step.

37. The filtering method according to claim 33, further comprising an external transmission step of transmitting each of the access requests determined not to be transmitted to the server in the pattern determination step, to a predetermined external device based on a predetermined external transmission rule.

38. The filtering method according to claim 33, further comprising a storage step of storing each of the access requests determined not to be transmitted to the server in the pattern determination step, in a predetermined storage medium based on a predetermined storage rule.

39. The filtering method according to claim 33, further comprising an update step of updating the illegal pattern database, the legal pattern database, the pattern estimation rule, the pattern determination rule, the external transmission rule, the storage rule, or a predetermined update rule, based on the predetermined update rule.

40. The filtering method according to claim 33, further comprising:

a statistic estimation step of referring to a statistically illegal request database which stores information on the access requests considered to be illegal accesses from the statistic of the access requests for the server, and estimating the legality of each of the access requests based on a predetermined statistic estimation rule;

a statistic determination step of determining whether the access request is to be transmitted to the server based on the estimation in the estimation step and on a predetermined determination rule; and

an access request transmission step of transmitting, as a legal access request, only the access request determined to be transmitted to the server in the pattern and statistic determination steps, to the server.

41. The filtering method according to claim 40, wherein

the statistically illegal request database stores transmitting end information on the clients each of which issues access requests, the number of which exceeds a predetermined number within a predetermined time, among the clients who transmit the access requests to the server;

the statistic estimation step includes estimating that each of the access requests is the illegal access if the transmitting end information on the access request corresponds to any one of the transmitting end information stored in the statistically illegal request database, and estimating that the access request is the legal access if the transmitting end information on the access request does not correspond to any one of the transmitting end information stored in the statistically illegal request database; and

the statistic determination step includes determining that the access request estimated as the illegal access in the statistic estimation step is not to be transmitted to the server, and determining that the access request estimated as the legal access in the statistic estimation step is to

be transmitted to the server.

42. The filtering method according to claim 40, wherein the statistically illegal request database stores request contents of the access requests, the number of which exceeds a predetermined number within a predetermined time, among the request contents of the access requests transmitted to the server;

the statistic estimation step includes estimating that each of the access requests is the illegal access if the request content of the access request corresponds to any one of the request contents stored in the statistically illegal request database, and estimating that the access request is the legal access if the request content of the access request does not correspond to any one of the request contents stored in the statistically illegal request database; and

the statistic determination step includes determining that the access request estimated as the illegal access in the statistic estimation step is not to be transmitted to the server, and determining that the access request estimated as the legal access in the statistic estimation step is to be transmitted to the server.

43. The filtering method according to claim 40, wherein the statistically illegal request database stores transmitting end information on the clients each of which issues access requests, the number of which exceeds a predetermined number within a predetermined time, among the clients who transmit the access requests to the server, and stores request contents of the access requests, the number of which exceeds a predetermined number within a predetermined time, among the request contents of the access requests transmitted to the server;

the statistic estimation step includes estimating that each of the access requests is the illegal access if the transmitting end information on the access request corresponds to any one of the transmitting end information stored in the statistically illegal request database, or if the request content of the access request corresponds to any one of the request contents stored in the statistically illegal request database, and estimating that the access request is the legal access if the transmitting end information on the access request does not correspond to any one of the transmitting end information stored in the statistically illegal request database, and if the request content of the access requests does not correspond to any one of the request contents stored in the statistically illegal request database; and

the statistic determination step includes determining that the access request estimated as the illegal access in the statistic estimation step is not to be transmitted to the server, and determining that the access request estimated as the legal access in the statistic estimation step is to be transmitted to the server.

44. The filtering method according to claim 40, wherein

the statistically illegal request database stores transmitting end information on the clients each of which issues access requests, the number of which exceeds a predetermined number within a predetermined time, among the clients who transmit the access requests to the server, and stores request contents of the access requests, the number of which exceeds a predetermined number within a predetermined time, among the request contents of the access requests transmitted to the server;

the statistic estimation step includes calculating a predetermined estimation value according to a degree to which the transmitting end information on each of the access requests and the request content of the access request correspond to the transmitting end information and request contents stored in the statistically illegal request database, respectively; and

the statistic determination step includes comparing

the estimation value calculated in the statistic estimation step with a predetermined threshold value, and determining whether the access request is to be transmitted to the server.

45. The filtering method according to claim 40, wherein the statistic estimation step includes estimating the legality of only the access request determined to be transmitted to the server in the pattern determination step.

46. The filtering method according to claim 40, wherein the pattern estimation step includes estimating the legality of only the access request determined to be transmitted to the server in the statistic determination step.

47. The filtering method according to claim 40, wherein the predetermination step includes predetermining whether only the access request, determined to be transmitted to the server in the statistic determination step, corresponds to any one of the legal access patterns stored in the legal pattern database.

48. The filtering method according to claim 40, further comprising an external transmission step of transmitting the access requests which are not transmitted to the server in the access request transmission step, to the predetermined

external device based on a predetermined external transmission rule.

49. The filtering method according to claim 40, further comprising a storage step of storing the access requests which are not transmitted to the server in the access request transmission step, to the predetermined storage medium based on a predetermined storage rule.

50. The filtering method according to claim 40, further comprising an update step of updating the statistically illegal request database, the statistic estimation rule, the statistic determination rule, the external transmission rule, and at least one of the storage rule and a predetermined update rule, based on at least one of the predetermined update rule and the statistic of the access requests to the server.

51. The filtering method according to claim 50, wherein the update step includes any one or both of addition and deletion of at least one of the transmitting end information and the request contents stored in the statistically illegal request database, according to any one or both of the number of access requests for each client who transmits the access requests to the server within a predetermined time and the number of access requests for

each request content of the access requests transmitted to the server within a predetermined time.

52. The filtering method according to claim 33, further comprising:

a response estimation step of referring to an illegal response database which stores patterns of illegal responses that should not be transmitted to each of the clients, among the responses transmitted from the server to each of the clients as the service according to the respective access requests, and estimating the legality of each of the responses based on the predetermined response estimation rule;

a response determination step of determining whether the response is to be transmitted to the client based on an estimation in the response estimation step and on the predetermined response determination rule; and

a response transmission step of transmitting, as a legal response, only the response determined to be transmitted to the client in the response determination step, to the client.

53. The filtering method according to claim 52, wherein the response estimation step includes estimating that the response is an illegal response if the response

corresponds to any one of the illegal response patterns stored in the illegal response database, and estimating that the response is a legal response if the response does not correspond to any one of the illegal response patterns stored in the illegal response database; and

the response determination step includes determining that the response estimated as the illegal response in the response estimation step, is not to be transmitted to the client, and determining that the response estimated as the legal response in the response estimation step, is to be transmitted to the client.

54. The filtering method according to claim 52, wherein

the response estimation step includes calculating a predetermined estimation value according to a degree to which the response corresponds to the illegal response patterns stored in the illegal response database; and

the response determination step includes comparing the estimation value calculated in the response estimation step with a predetermined threshold value, and determining whether the response is to be transmitted to the client.

55. The filtering method according to claim 52, further comprising an external transmission step of transmitting at least one of the response which is not transmitted to

the client in the response transmission step and the access request causing the response, to a predetermined external device based on a predetermined external transmission rule.

56. The filtering method according to claim 52, further comprising a storage step of storing at least one of the response which is not transmitted to the client in the response transmission step and the access request causing the response, in the predetermined storage medium based on a predetermined storage rule.

57. The filtering method according to claim 52, further comprising an update step of updating the illegal response database, the response estimation rule, the response determination rule, the external transmission rule, at least one of the storage rule and a predetermined update rule, based on the predetermined update rule.

58. The filtering method according to claim 33, further comprising an access request decryption step of decrypting an access request which has been subjected to a predetermined encryption processing, wherein

the pattern estimation step, the predetermination step, or the statistic estimation step includes estimating or determining the access request decrypted in the access

request decryption step.

59. The filtering method according to claim 58, further comprising:

transmitting not the access request decrypted in the access request decryption step but the access request which has been subjected to the predetermined encryption processing, to the server if only the legal access request among the access requests is to be transmitted to the server.

60. The filtering method according to claim 58, further comprising a response decryption step of decrypting a response which has been subjected to a predetermined encryption processing, wherein

the response estimation step includes estimating the response decrypted in the response decryption step.

61. The filtering method according to claim 60, further comprising:

transmitting not the response decrypted in the response decryption step but the response which has been subjected to the predetermined encryption processing, to the client if only the legal response among the responses is to be transmitted to the client.

62. The filtering method according to claim 33, further comprising:

a pseudo-response creation step of referring to a pseudo-response database which stores pseudo-responses corresponding to the patterns of the illegal accesses to the server, respectively, and each indicating that the corresponding illegal access is successful or successfully proceeding, and creating pseudo-responses corresponding to the patterns of the access requests, each of which is determined as the illegal access and is not transmitted to the server, respectively; and

a pseudo-response transmission step of transmitting the pseudo-responses created in the pseudo-response creation step to the clients, respectively.

63. The filtering method according to claim 33, further comprising:

a decoy step of receiving the access requests each of which is determined as the illegal access and is not transmitted to the server, and creating, as a decoy of the sever, pseudo-responses each indicating that the corresponding illegal access is successful or successfully proceeding; and

a pseudo-response transmission step of transmitting the pseudo-responses created in the decoy step to the clients,

respectively.

64. The filtering method according to claim 33, further comprising:

a pseudo-response creation step of referring to a pseudo-response database which stores pseudo-responses corresponding to the patterns of the illegal accesses to the server, respectively, and each indicating that the corresponding illegal access is successful or successfully proceeding, and creating pseudo-responses corresponding to the illegal access patterns stored in the pseudo-response database among the access requests each of which is determined as the illegal access and is not transmitted to the server;

a decoy step of receiving the access requests which do not correspond to the illegal access patterns stored in the pseudo-response database among the access requests each of which is determined as the illegal access and is not transmitted to the server, and creating, as a decoy of the sever, pseudo-responses each indicating that the corresponding illegal access is successful or successfully proceeding; and

a pseudo-response transmission step of transmitting the pseudo-responses created in the pseudo-response creation step or the decoy step to the clients, respectively.

65. A computer program containing instructions which when executed on a computer causes the computer to perform a filtering method used on a client and a server providing a service in accordance with each of access requests from the client, and which transmits only a legal access request among the access requests to the server, the filtering method comprising:

a pattern estimation step of referring to an illegal pattern database which stores patterns of illegal accesses to the server, and estimating legality of each of the access requests based on the illegal access patterns referred to and on a predetermined pattern estimation rule; and

a pattern determination step of determining whether each of the access requests is to be transmitted to the server based on an estimation result at the pattern estimation step and on a predetermined pattern determination rule.